

**UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
CASE NO. 20-CV-954-WO-JLW**

FARHAD AZIMA,)
)
)
Plaintiff,)
)
v.)
)
NICHOLAS DEL ROSSO and)
VITAL MANAGEMENT SERVICES,)
INC.,)
)
Defendants.)

**DEFENDANTS' RESPONSE
TO PLAINTIFF'S OBJECTIONS TO ORDER AND RECOMMENDATION
ON DEFENDANTS' MOTION TO DISMISS PURSUANT TO RULE 12(b)(6)**

INTRODUCTION

The Magistrate Judge was correct to recommend dismissal of seven of Plaintiff Farhad Azima's causes of action. This case arises from an incident in or before 2016 in which Azima alleges that foreign non-parties acquired access to his email account. Azima (wrongly) blames Defendants for orchestrating this alleged incident and, as the Magistrate Judge held, has failed to "adequately allege[] an agreement between Defendants" and the purported primary hacker. Dkt. 54 ("O&R") at 32. The seven causes of action at issue here do not fit the facts alleged.

Azima's Wiretap Act claims are misplaced because that Act gives a cause of action only against the primary actor, while Defendants are alleged to have hired one of the third parties. Beyond that, these claims are time-barred, improperly extraterritorial, and ill-founded because the Act only applies to intercepting live transmissions.

As for Azima's computer trespass and conversion claims, the Magistrate Judge was correct to conclude that they are time-barred and not subject to equitable tolling. Azima's barebones complaint omits facts that satisfy the elements of

identity theft, publication of personal information, or the North Carolina Unfair and Deceptive Trade Practices Act. The Court should sustain the recommendation as to dismissal of the seven counts at issue.

BACKGROUND

Defendants' Partial Objection, Dkt. 57 ("Defs' Obj.") at 2-3, sets forth the background to this case, and its statement of facts is incorporated here by reference. As noted there - and as Azima admits on the first page of his objection - Azima has known of the alleged hacking incident at issue in this case since at least September 2016, when he filed litigation with hacking allegations identical to those here. See *id.*; see also Dkt. 56 ("Obj.") at 1.

Azima filed this action against Defendants more than four years later, on October 15, 2020, alleging that Defendants helped organize the alleged hacking effort on RAKIA's behalf. Dkt. 1 ("Compl.") ¶¶ 1-2, 7. Azima asserted eleven causes of action under federal and state law. See *id.* ¶¶ 44-139.

Defendants moved to dismiss all claims, arguing that Azima's claims were time-barred and that he failed to state a claim as to any of them. See Dkt. 32 ("Mot.") at 7-10, 16-

26. On August 9, 2021, the Magistrate Judge appropriately recommended the dismissal of seven of Azima's eleven causes of action: two as time-barred (Count IV (computer trespass) and Count V (conversion)), and five for failure to state a claim under applicable substantive law (Counts I and II (Wiretap Act and conspiracy to violate it), Count VI (identity theft), Count VII (publication of personal information), and Count IX (North Carolina Unfair and Deceptive Trade Practices Act). O&R 1, 10, 17-21, 25-28, 29-30. Azima objects to the Magistrate Judge's recommendation of dismissal as to those counts. For the reasons that follow, this Court should dismiss those seven counts consistent with the Magistrate Judge's recommendation.

ARGUMENT

I. This Court Should Adopt the Magistrate Judge's Recommendation to Dismiss Azima's Wiretap Claims.

A. There Is No Secondary Liability under the Wiretap Act (Count I).

The Magistrate Judge correctly concluded that Azima's Wiretap Act claims, at best, assert that Defendants are liable for procuring a violation of that Act by another, and that

the Wiretap Act does not create a cause of action for "secondary" liability of this sort. O&R 18-20.¹

The Wiretap Act gives a cause of action against "the person" who committed "th[e] violation" of "intercept[ing]" the relevant communications. 18 U.S.C. § 2520(a). An earlier version of the statute allowed a suit against anyone who "procures any other person to intercept . . . such communications." Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 801, 82 Stat. 197, 223 (1968) (enacting former 18 U.S.C. § 2520). But in 1986, as the Magistrate Judge concluded and as courts have broadly recognized, Congress eliminated that theory of liability by striking the word "procures" from the civil liability provision of the statute. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 103, 100 Stat. 1848, 1853-54 (1986); see O&R 18-19; *Kirch v. Embarq Mgmt. Co.*, 702 F.3d 1245, 1247 (10th

¹ Azima pleads Count I as a "disclosure" claim under 18 U.S.C. §§ 2511(1)(c) and 2520, Compl. at 12, and Count II as a "conspiracy to disclose and use" claim under 18 U.S.C. §§ 2511(1)(d) and 2520 and 18 U.S.C. § 371, *id.* at 15. Defendants address these Counts in turn, as the Magistrate Judge did. O&R 17-21.

Cir. 2012); *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 169 (5th Cir. 2000); see also, e.g., *Motise v. Am. Online, Inc.*, 2005 WL 1667658, at *4 (E.D. Va. June 24, 2005) (Wiretap Act “does not recognize a cause of action for aiding and abetting a primary violator”); *Buckingham v. Gailor*, 2001 WL 34036325, at *6 (D. Md. Mar. 27, 2001), *aff’d*, 20 F. App’x 243 (4th Cir. 2001).

Azima cites two cases that he says support a conclusion that the statute still allows a suit for “procuring,” but then makes no effort to explain why this Court should follow that outlier view. The majority view adopted by the Magistrate Judge is correct: Congress changed the statutory text, and courts are required to presume that Congress intends a change when it makes a change, *Stone v. INS*, 514 U.S. 386, 397 (1995). Only the majority view makes sense of the change that Congress made, by giving effect to Congress’s removal of the “procuring” language. This Court should follow the cogent analysis laid out in, among other decisions, the opinions of the Tenth and Fifth Circuits in *Kirch* and *Peavy*.

As for Azima's cases, *Lonegan v. Hasty*, 436 F. Supp. 2d 419, 428 (E.D.N.Y. 2006), stated in *dicta* that Congress appeared to have been meaning to make only a ministerial change, but that is error because it ignores the presumption that Congress means its changes to have effect. See *Shefts v. Petrakis*, 954 F. Supp. 2d 769, 776-77 (C.D. Ill. 2013) (observing that the *Lonegan* court's interpretation is "merely *dicta*" and granting summary judgment to defendant on procurement, conspiracy and secondary theories of liability). The court's conclusion was not necessary to its decision in any event, because the court went on to conclude that the complaint at issue pleaded a direct Wiretap Act claim after all and thus would survive dismissal whether or not a claim for secondary liability would be permitted. As for the unpublished decision in *Boseovski v. McCloud Healthcare Clinic, Inc.*, 2020 WL 68578, at *5-6 (E.D. Cal. Jan. 7, 2020), that addressed the special case of corporate *respondeat superior* liability and whether the statute's reference to an "entity" being potentially liable implied that the act of an employee could be attributed to a corporate employer. The court was not asked to decide, and did not hold, that a defendant (like

Defendants here) could be held responsible for procuring acts by a third party notwithstanding Congress's amendment to the statute.

To avoid the secondary liability problem, Azima principally urges here in his objection that his Count I actually states a claim that Defendants themselves disclosed knowingly-hacked data. Obj. 5-7. But as the Magistrate Judge rightly observed, the complaint factually alleges that Defendants "directed" a third party to post his hacked data on the Internet, which is a theory of secondary liability, not primary. O&R 17-20; Compl. ¶¶ 49, 51-52. Azima's conclusory allegations that Defendants *themselves* "intercepted" or "disclosed" his data are contradicted by the specific factual allegation that it was a third party (non-party CyberRoot Risk Advisory Private Ltd. ("CyberRoot")) that did this, not Defendants; as the Magistrate Judge determined, these conclusory allegations "lack the particularity required to state a plausible claim for relief and conflict with other more specific allegations in the complaint attributing this conduct to CyberRoot." O&R 19-20 n.6; see *Herzer v. Redstone*, 2018 WL 5094933, at *7 (C.D. Cal. July 10, 2018) (dismissing

conclusory complaint “devoid . . . of any factual allegations” of specific violations of the Wiretap Act).²

B. The Wiretap Act Does Not Support Conspiracy Liability (Count II).

Count II asserts a claim for “[c]onspiracy” under the Wiretap Act and 18 U.S.C. § 371, the federal criminal conspiracy statute. The Magistrate Judge correctly concluded that this count should be dismissed because § 371 does not create a cause of action for civil liability. O&R 20-21.³ In his objection, Azima does not address or defend his assertion of a “conspiracy” claim under § 371, which is fatal

² Azima’s objection refers to material beyond the complaint, including a witness statement by one of the Defendants. See Obj. 6. That testimony – which among other things includes a categorical denial that Defendants were involved in the hacking – does not support his argument, so it is not material. Given it is not part of the complaint and is not judicially noticeable, the reference to it is improper and should be disregarded on this 12(b)(6) motion.

³ The cases uniformly so hold. See, e.g., *Andrews v. Heaton*, 483 F.3d 1070, 1076 (10th Cir. 2007) (affirming dismissal of 18 U.S.C. § 371 claim because it is a criminal statute that does not provide a private right of action); *Rockefeller v. Rehnquist*, 2004 WL 210649, at *1 (D.C. Cir. Jan. 30, 2004) (same); *Sanders v. GNC Holdings, Inc.*, 2020 WL 5792462, at *3 (E.D.N.C. July 8, 2020), report and recommendation adopted, 2020 WL 5770851 (E.D.N.C. Sept. 28, 2020) (same); *Bey ex rel Graves v. Richmond Redevelopment & Hous. Auth.*, 2013 WL 4066945, at *5 (E.D. Va. Aug. 9, 2013) (same).

to his position. The Court should, therefore, adopt the Magistrate Judge's recommendation to dismiss Count II.

Azima now urges that Count II should be sustained because, he says, this Count is where he alleges that Defendants "used" the allegedly intercepted material under 18 U.S.C. § 2511(1)(d). Azima did not present this argument in his original opposition brief, so it is waived. *See, e.g., Elliott v. Oldcastle Lawn & Garden, Inc.*, 2017 WL 1206408, at *3 (D.S.C. Mar. 31, 2017) (arguments not raised before magistrate judge are waived). Azima is also wrong, because Count II merely alleges that Defendants participated in a conspiracy to use intercepted data, not that Defendants themselves made direct use of that data. *See, e.g.,* Compl. ¶ 55 (alleging that Defendants "knowingly agreed and conspired with" others to disclose the data (emphasis added)). As discussed above, the Wiretap Act creates a cause of action only against a primary actor, not "procurers" or other third parties. The Magistrate Judge was therefore correct to recommend dismissal of Count II.

C. Azima's Wiretap Claims are Untimely, Improperly Extraterritorial, and Lack a Predicate Interception.

Azima's Wiretap claims fail for three other reasons. First, as discussed in Defendants' own objection, Azima was plainly on notice of the alleged hacking four years ago when he brought a lawsuit over it. Defs' Obj. 14-17. If the Court agrees with Defendants' objection and takes judicial notice of Azima's September 2016 hacking complaint, that will be fatal to the Wiretap claims too because they have a two-year limitations period. 18 U.S.C. § 2520(e); Mot. 7-10.

Indeed, Azima's very objection itself offers an independent basis for determining the 2016 accrual date of Azima's claims, and so bolsters Defendants' time-bar argument, because Azima concedes that he was hacked in "2016" and "immediately brought suit for the hacking in the United States." Obj. 1. A court's power to rely "upon facts conceded by counsel is as plain as its power to act upon the evidence produced." *Oscanyan v. Arms Co.*, 103 U.S. 261, 263 (1880). The 2016 filing date of Azima's prior hacking suit, which Azima here concedes, is the latest possible date for the accrual of this cause of action (as well as those addressed

in Defendants' objection, and below). See, e.g., *Allen v. AstraZeneca Pharms. LP*, 2015 WL 4749146, at *2 (E.D.N.C. Aug. 11, 2015) (filing date of a prior nearly identical suit was the latest possible accrual date for limitations period). The Wiretap claims are therefore time-barred.

Second, the Wiretap Act does not apply extraterritorially, and so does not reach the conduct here, which allegedly took place in India. See *Huff v. Spaw*, 794 F.3d 543, 547 (6th Cir. 2015) (holding that determining whether the conduct is extraterritorial depends on where the interception took place); *United States v. Maturo*, 982 F.2d 57, 60 (2d Cir. 1992) (noting that Title III, 18 U.S.C. §§ 2510-2520, does not apply outside the United States); *Zheng v. Yahoo! Inc.*, 2009 WL 4430297, at *3-4 (N.D. Cal. Dec. 2, 2009) (dismissing Wiretap claims based on purported interception that took place in China because statute does not apply extraterritorially).

Here, the complaint alleges that servers located in India and belonging to an Indian company (non-party BellTroX Info Tech Services) were used to hack Azima. Compl. ¶ 2-3, 16, 49. As the Magistrate Judge held – and Azima does not contest

- the Complaint does "not adequately allege[] an agreement between Defendants and BellTroX." O&R 32. Instead, Azima contends that another Indian company (non-party CyberRoot) "disclosed Azima's stolen data on internet blog sites they created" from India, see *id.* ¶¶ 6, 19-22. Because the alleged hacking and disclosure did not occur in the United States, the Wiretap Act does not reach this conduct.

Third, Azima fails to plead a qualifying "interception," which is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication." 18 U.S.C. § 2510(4). To be actionable under the Wiretap Act, a communication must be intercepted in real time, during transmission. See *Boudreau v. Lussier*, 901 F.3d 65, 76-78 (1st Cir. 2018) (collecting cases).⁴ An email is not "intercepted" when it is obtained from "electronic storage." *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 951 (N.D. Cal.

⁴ See also, e.g., *Gamrat v. McBroom*, 822 F. App'x 331, 334 (6th Cir. 2020); *United States v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir. 2003).

2014) (citations omitted).⁵ Azima alleges that the Indian non-parties obtained his account passwords and downloaded his emails from his account, Compl. ¶¶ 6, 17, 51, 55; he nowhere alleges that they were intercepted in transit.

The Court should dismiss Counts I and II on these additional grounds.

II. This Court Should Adopt the Magistrate Judge's Recommendation to Dismiss Azima's State Law Claims.

A. Azima's Computer Trespass and Conversion Claims Are Time-Barred.

The Magistrate Judge properly concluded that Azima's computer trespass and conversion claims are time-barred. O&R 10-13. Azima admitted below that the one-year limitations period for computer trespass would render that claim untimely absent tolling, Dkt. 34 ("Opp.") at 6-7; Dkt. 39 ("Reply") at 6, and does not dispute the Magistrate Judge's conclusion that his conversion claim "accrue[d]" when the hacking occurred in 2016 or that that claim has a three-year limitations

⁵ See also, e.g., *Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631, 634, 638-39 (E.D. Va. 2009) (no "interception" where husband accessed wife's emails stored in the "destination server").

period. O&R 12-13 (quotations omitted). He objects only by contending that equitable estoppel should save these claims. Obj. 10-15.

The Magistrate Judge was correct, however, that Azima failed to plead what equitable estoppel requires: "specific allegations explaining how he relied upon Defendant's false statements to his detriment." O&R 16.⁶ Azima suggests that he is automatically entitled to tolling because spear-phishing emails are "inherently deceptive" and "disguise[]" the hacker's identity. Obj. 12. That is not the law.⁷ As other

⁶ *Bankaitis v. Allstate Insurance Co.*, 229 F. Supp. 3d 381, 387 (M.D.N.C. 2017), did not dispense with any requirement that a plaintiff plead facts to support tolling (*contra* Obj. 14). The court there simply found that the plaintiff's factual allegations were adequate, because they showed an effort to induce the plaintiff to delay making a claim. *Id.* What Azima quotes is a description of the defendant's argument that the complaint lacked such allegations, not the court's holding.

⁷ Neither *Friedland v. Gales*, 131 N.C. App. 802, 807 (1998), nor *Hatcher v. Flockhart Foods, Inc.*, 161 N.C. App. 706, 707-08 (2003), on which Azima relies, dealt with equitable tolling for spear-phishing claims. Obj. 10-12. In *Friedland*, the defendant was equitably estopped in a wrongful death case because he affirmatively concealed his involvement by lying to the police and blaming someone else for the murder. 131 N.C. App. at 803-05, 808. *Hatcher* dealt with an insurance company that misled a plaintiff as to the responsible party for the tort, leading plaintiff to sue the wrong

courts have explained, even though “the investigation necessary to uncover the hacker's identity may be substantial,” that does not excuse a plaintiff from timely filing claims. *Sewell v. Bernardin*, 795 F.3d 337, 342 (2d Cir. 2015). The plaintiff “must . . . discover the hacker’s identity within” the limitations period “to avoid dismissal.” *Id.*

Azima’s second argument for tolling is his conclusory allegation that Defendant Del Rosso and others gave false testimony in 2020 during Azima’s fraud trial in England, which was “designed to conceal” the “Defendants’ role in the hacking.” Obj. 13-14.⁸ But as the Magistrate Judge observed, the 2020 trial happened after the limitations period had already expired, O&R 15-16, so cannot have prejudiced Azima. See *Caviness v. Derand Res. Corp.*, 983 F.2d 1295, 1302 (4th Cir. 1993) (no equitable estoppel where plaintiff’s claims

tortfeasor within the limitations period. 161 N.C. App. at 710-12.

⁸ Azima misstates the case law in suggesting, Obj. 12, that statements by “related parties” can estop a defendant from raising a statute of limitations defense. His cited case applies to the statements of a defendant’s agent. *Hatcher*, 161 N.C. App. at 708. Azima does not point to statements by any person alleged to be an agent of Defendants.

had "already been barred at the time of the" alleged misrepresentation); *Teague v. Randolph Surgical Assocs., P.A.*, 129 N.C. App. 766, 772 (1998) (similar).

Finally, Azima suggests, Obj. 13, that Del Rosso and RAKIA's lawyer "created a false evidentiary trail" by sending emails between themselves that "purported to 'break the news' of the discovery of the hacked material on websites," Compl. ¶ 35. But as the Magistrate Judge found, because these emails were not sent to Azima, they cannot have "prevented him from filing suit against Defendants within the limitations period." O&R 15. The claims are time-barred, and the Magistrate Judge was correct to recommend dismissal.⁹

B. Azima Fails to State a Claim for Identity Theft (Count VI).

The Magistrate Judge properly concluded that Azima failed to state a claim for identity theft under N.C. Gen. Stat. §§ 14-113.20 and 1-539.2C. The underlying criminal statute applies when the defendant impersonates another person, and

⁹ These claims should also be dismissed for the additional reasons set out in Defendants' Motion to Dismiss. Mot. 22-23; Reply 12-13.

Azima's allegations never accuse Defendants of pretending to be Azima. O&R 25-26. Azima's suggestion that "Defendants had access to Azima's passwords through CyberRoot" and so it is "plausible" that they used them, merely highlights that he has not alleged that they did so. Obj. 16-17. The Magistrate Judge's conclusion that he "cannot identify specific factual allegations in the complaint demonstrating that Defendants made representations to any other individual or entity that they were Plaintiff," O&R 26, is correct and should be adopted.

C. Azima Fails to State a Claim for Publication of Personal Information (Count VII).

The Magistrate Judge was similarly correct to conclude that Azima's publication of personal information claim should be dismissed because Azima failed to allege that he previously objected to the disclosure of any such information or that Defendants had "actual knowledge" of such an objection, which is required to state a claim. See O&R 26-28; N.C. Gen. Stat. § 75-66(a). Azima argues that his hacking defense in the English Proceedings counts as notice, but the Magistrate Judge was right that it does not because Defendants were not

party to those proceedings. *Id.* 27-28. Azima's suggestion that the Court can just assume that the Defendants knew of the lawsuit and would have inferred that Azima objected to the publication of his information is wrong, and Azima cites no law to support it. Obj. 18-19.

Azima also cites no authority to support his argument – advanced for the first time here – that because certain allegedly stolen materials were marked “confidential” he does not have to plead facts suggesting that he gave Defendants notice of his objection to the disclosure. Obj. 18. This argument is waived here because it was not presented to the Magistrate Judge. *See Elliott*, 2017 WL 1206408, at *3. Anyway, there is no authority to suggest the mere marking of documents as confidential excuses a plaintiff from pleading a sufficient objection to publication and that Defendants had actual knowledge of such objection. *See* N.C. Gen. Stat. § 75-66; *In re Winter*, 2015 WL 5063953, at *3 (Bankr. E.D.N.C. Aug. 26, 2015). This Court should adopt the recommendation of the Magistrate Judge to dismiss Count VII for failure to state a claim.

D. Azima Fails to State a UDTP Act Claim (Count IX).

Finally, the Magistrate Judge properly concluded that Azima failed to state a claim under the North Carolina Unfair and Deceptive Trade Practices ("UDTP") Act because he has alleged neither commercial dealings nor a competitor relationship between himself and Defendants, nor injury to consumers as required when a business (as opposed to a consumer) seeks to state a UDTP claim. O&R 30. Azima is wrong that merely alleging that Defendants generally transacted in commerce is sufficient to satisfy this requirement.

As the Magistrate Judge correctly observed, the UDTP Act is "intended to 'regulate two types of interactions in the business setting: (1) interactions between businesses, and (2) interactions between businesses and consumers,'" and "North Carolina courts 'have viewed the rights of businesses to sue other businesses for violations of the UD[T]PA' with a much more skeptical eye." O&R 29-30 (citing *McClean v. Duke Univ.*, 376 F. Supp. 3d 585, 608 (M.D.N.C. 2019); *Exclaim Mktg., LLC v. DirecTV, LLC*, 134 F. Supp. 3d 1011, 1020 (E.D.N.C. 2015), *aff'd*, 674 F. App'x 250 (4th Cir. 2016); and *Dalton v. Camp*, 353 N.C. 647, 655 (2001)). As a result, the

UDTP Act does not cover "all wrongs in a business setting." *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, 194 F.3d 505, 519 (4th Cir. 1999). It only provides a non-consumer plaintiff with a cause of action against another business where the parties are engaged in commercial dealings or are business competitors. O&R 30; see also *White v. Thompson*, 364 N.C. 47, 51-52 (2010) (breach of fiduciary duties by plaintiffs' partner did not occur "in or affecting commerce").

Here, Azima admits both that his complaint lacks any such allegations, and that he could not make this allegation as to Defendants – he claims only that he could amend his complaint to allege that RAKIA (who is not a party here) was a former business partner. Obj. 20 n.8. Azima also concedes that he has not pled damage to the consuming public by reiterating only the harm to him personally and "his reputation." Obj. 20.¹⁰ As a result, this claim fails, and this Court should

¹⁰ Azima's UDTP Act claim also fails because he has not sufficiently alleged an "unfair or deceptive act or practice" as explained in Defendants' Motion to Dismiss. Mot. 25; Reply 14. The decisions Azima cites do not counsel a different result: in fact, both dismissed the plaintiff's UDTP Act claim. See Obj. 20 (citing *Prince v. Wright*, 141 N.C. App. 262, 269 (2000) (affirming dismissal of plaintiff's UDTP Act

adopt the recommendation of the Magistrate Judge to dismiss Count IX for failure to state a claim.

III. In the Alternative, Azima's Claims Are Time-Barred.

Beyond the points on which the Magistrate Judge relied, this Court should also dismiss the claims here for the reasons set forth in Defendants' Motion, Mot. 7-9; Reply 2-5, as well as the Partial Objection, Defs' Obj. 6-17.

Azima's identity theft and publication of personal information claims "must be brought within three years from the date on which the identity of the wrongdoer was discovered or reasonably should have been discovered." N.C. Gen. Stat. §§ 75-66(e); 1-539.2C(c). His UDTP Act claim has a four-year limitations period, which begins when the alleged violation occurs. N.C. Gen. Stat. § 75-16.2; see also O&R 10. As explained in the Motion to Dismiss and Defendants' Partial Objection, Azima was aware of his hacking and disclosure claims no later than September 30, 2016, when he filed his

claim where the defendant's actions could not "be said to be 'in or affecting commerce'"); *Johnson v. Beverly-Hanks & Assocs., Inc.*, 328 N.C. 202, 209 (1991) (holding plaintiffs failed to establish any unfair or deceptive trade practice)).

lawsuit against RAKIA in Washington, D.C. See Mot. 4-5; Defs' Obj. 2-3. This Court may properly take judicial notice of the filing of that lawsuit for the purposes of adjudicating Defendants' statute of limitations defense. Defs' Obj. 6-17. Because Azima waited more than four years after filing that lawsuit to initiate this action, his claims are time-barred.

For the reasons set forth in Defendants' Partial Objection, Azima's conclusory suggestion that he did not discover Defendants' identity until August 28, 2020 is not sufficient to save his identity theft and publication of personal information claims. Reply 6; Defs' Obj. 15. The test is not just when the defendant's identity was discovered, but when it *reasonably should* have been discovered. See, e.g., *Hance v. First Citizens Bank & Tr. Co.*, 242 N.C. App. 251, at *5 (2015).

The same logic holds for Azima's UDTP claim. See *Avoki v. Carolina Telco Fed. Credit Union*, 2018 WL 3551524, at *2 (W.D.N.C. July 24, 2018), *aff'd*, 745 App'x 493 (4th Cir. 2018) (dismissing UDTP claim as time-barred where plaintiff "was well aware of and even threatened litigation" at the time of the purported UDTP violation but did not file suit until more

than four years later). Azima's conclusory allegations that an unidentified person posted new links to his material in 2018 and 2019 do not resuscitate his stale claim. These allegations are not sufficiently particularized to plead a "violation" and cannot revive his otherwise stale claims.

CONCLUSION

For these reasons, the Court should adopt the Magistrate Judge's recommendation to dismiss Counts I, II, IV, V, VI, VII and IX; and, for the further reasons stated in Defendants' Partial Objection, the Court should dismiss this action in its entirety.

Respectfully submitted this 7th day of September, 2021.

**NELSON MULLINS RILEY &
SCARBOROUGH, LLP**

By: /s/ Brandon S. Neuman
Kieran J. Shanahan, NCSB# 13329
Brandon S. Neuman, NCSB# 33590
Jeffrey M. Kelly, NCSB# 47269
Nathaniel J. Pencook, NCSB# 52339
Glenlake One
4140 Parklake Avenue, Suite 200
Raleigh, North Carolina, 27612
Telephone: (919) 329-3800
Facsimile: (919) 329-3799
kieran.shanahan@nelsonmullins.com
brandon.neuman@nelsonmullins.com
jeff.kelly@nelsonmullins.com
nate.pencook@nelsonmullins.com
Counsel for Defendants

WORD COUNT CERTIFICATION

Pursuant to Local Rule 72.4, I hereby certify, subject to Fed. R. Civ. P. 11, that the accompanying brief contains 4,383 words, according to the word count feature of the word processing system used to prepare the brief. Accordingly, the brief does not exceed the 6,250 word limitation.

Respectfully submitted this 7th day of September, 2021.

**NELSON MULLINS RILEY &
SCARBOROUGH, LLP**

By: /s/ Brandon S. Neuman
Kieran J. Shanahan, NCSB# 13329
Brandon S. Neuman, NCSB# 33590
Jeffrey M. Kelly, NCSB# 47269
Nathaniel J. Pencook, NCSB# 52339
Glenlake One
4140 Parklake Avenue, Suite 200
Raleigh, North Carolina, 27612
Telephone: (919) 329-3800
Facsimile: (919) 329-3799
kieran.shanahan@nelsonmullins.com
brandon.neuman@nelsonmullins.com
jeff.kelly@nelsonmullins.com
nate.pencook@nelsonmullins.com
Counsel for Defendants

CERTIFICATE OF SERVICE

I hereby certify that on this 7th day of September, 2021, I electronically filed the foregoing **Defendants' Response To Plaintiff's Objections to Order and Recommendation on Defendants' Motion to Dismiss Pursuant to Rule 12(b)(6)** with the Clerk of the Court using the CM/ECF system, which will send electronic notification of filing to the following:

Jonathan Townsend
Christopher W. Jones
Ripley Rand
Womble Bond Dickinson (US) LLP
555 Fayetteville Street
Suite 1100
Raleigh, NC 27601
jonathan.townsend@wbd-us.com
ripley.rand@wbd-us.com
chris.jones@wbd-us.com

Calvin Lee
Ian Herbert
Brian Hill
Kirby D. Behre
Miller & Chevalier Chartered
900 16th Street, NW
Washington, D.C. 20006
cllee@milchev.com
iherbert@milchev.com
bhill@milchev.com
kbehre@milchev.com

**NELSON MULLINS RILEY &
SCARBOROUGH, LLP**

By: /s/ Brandon S. Neuman
Kieran J. Shanahan, NCSB# 13329
Brandon S. Neuman, NCSB# 33590
Jeffrey M. Kelly, NCSB# 47269
Nathaniel J. Pencook, NCSB# 52339
Glenlake One
4140 Parklake Avenue, Suite 200
Raleigh, North Carolina, 27612
Telephone: (919) 329-3800
Facsimile: (919) 329-3799
kieran.shanahan@nelsonmullins.com
brandon.neuman@nelsonmullins.com
jeff.kelly@nelsonmullins.com
nate.pencook@nelsonmullins.com
Counsel for Defendants